encrypted data and random data stored therein, said encrypted data having been encrypted according to an encryption key which is based on said random data, and wherein said random data is selected from a predetermined portion of a random file which is generated by a pseudo random generator and was recorded on predetermined regions on the same surface as the encrypted data on said storage area.--

--94. The recording medium according to claim 93, further comprising stored therein data indicative of the portion of said random file corresponding to said random data.--

--95. A recording medium comprising:

a storage area for storing data; and

encrypted data stored therein, said encrypted data having been encrypted by using a second encryption key, wherein said second encryption key is generated based on a first encryption and a third encryption key, said first encryption key which being based on key data which is recorded on predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data, and said third encryption key being independent of said first encryption key.--

REMARKS

In light of the above amendatory matter and remarks to follow, reconsideration and allowance of this application are requested. This Amendment is responsive to the Final Office Action in the parent case of August 6, 1998.

The Examiner's remarks in the last Official Action in the parent application have been carefully considered. In response, Applicants' representative believes that all of the claims in this application are allowable.

The Applicants have made numerous amendments to the specification. The amendments are indicated in the "mark-up" copy of the specification submitted herewith, and they include the revisions specified by the Examiner in an Office Action in the parent case. The amendments are made for purposes of clarification and they do not add any new matter to the application.

The drawings are corrected as requested in an Office Action in the parent case in accordance with the Request for Approval of Drawing Change submitted herewith.

In this Amendment, claims 60-95 have been added which are the same as claims 60, 63, 66-88, 96, 98, 102, 103 and 107-113 in the parent case.

In the Final Office Action of the parent case claims 69-87, 96 and 102 (which are now claims 65-83, 85 and 87) were rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 65, 76, 79, 85 and 87 have been rewritten to overcome the rejections. Therefore Applicants request that the rejection of these claims based upon 35 U.S.C. §112, second paragraph, be withdrawn.

Claims 107-113 (now claims 89-95) were rejected under 35 U.S.C. §112, first paragraph because the specification does not reasonable provide enablement for the "single means" claims. Claims 107-113 (now claims 89-95) were rejected under 35 U.S.C. §101 because they are non-statutory. These claims have been rewritten to overcome the rejections. Therefore Applicants request that the rejection of these claims based upon 35 U.S.C. §101, be withdrawn.

Claims 60, 63, 66-69, 80-88, 96, 98, 102, 103, 107, 108, 111 and 112 were rejected under 35 U.S.C. §102(b) as being anticipated by Narasimhalu et al. ('718). Claims 63, 66, 83, 84, 87, 88, 102, 103, 107 and 108 35 U.S.C. §102(e) as being anticipated by Kikinis ('947). Claims 63, 66, 88 and 107 are rejected under 35 U.S.C. §102(e) as being anticipated by

Kondo ('773). Claims 70-79 are rejected under 35 U.S.C. §103 as being unpatentable over Narasimhalu et al. ('718). In response, the rejections are traversed for the following reasons.

Applicants' invention as recited in rewritten independent claim 60 requires generating an encryption key based on data which is "recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data." Applicants' claims therefore require that the data on which the encryption is based be recorded on the surface of the disk. Also, the data must be recorded on the same surface of the disk.

Narashimhalu et al. merely discloses using selected defects in the disk surface and not data recorded on the disk to encrypt information on the disk. Kondo merely discloses to record encrypting information on the edge of the disk. Kikinis merely discloses selectively obliterating the readability of bits in addressable sectors to encode data. None of the cited references teach or suggest the above features of the present invention. Therefore, withdrawal of the rejections are respectfully requested. If the Examiner does not withdraw the rejections, the Examiner is requested to identify those elements of the references which support his rejections.

Independent claims 61-62, 65, 76, 79, 84-89, 91, 93 and 95 include limitations corresponding to independent claim 60, and will not be analyzed to avoid repeating the above analysis. It is apparent, however, that claims 61-62, 65, 76, 79, 84-89, 91, 93 and 95 are distinguishable over the prior art for the same reasons as claim 1 discussed hereinabove.

Due to their dependency, claims 66-75, 77-78, 80-83, 90, 92 and 95 incorporate all of the limitations of the independent claims including the above-discussed features. It is apparent, therefore, that dependent claims 66-75, 77-78, 80-83, 90, 92 and 95 are, at a minimum, distinguishable over the prior art for the same reasons as Applicants' independent claims.

In light of the above, Applicants' representative traverses the Examiner's rejections and respectfully submits that the references, alone or in combination do not teach or suggest all of the features of the present invention, as claimed. In view of the foregoing amendments and remarks, it is believed that all of the claims now in this application are patentable over the prior art. Early and favorable consideration thereof is solicited. On the basis of the above amendments and remarks, reconsideration and allowance of this application are respectfully requested.

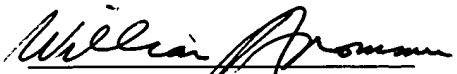
The above statements concerning the disclosures in the cited references represent the present opinion of Applicants' representative and, in the event that the Examiner disagrees, Applicants' representative respectfully requests the Examiner specifically indicate those portions of the respective references providing the basis for a contrary view.

Applicants' representative agrees with the Examiner that the prior art made of record and not relied upon is not as relevant to the claimed invention as are the references upon which the Examiner has relied.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number listed below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully submitted,
FROMMER LAWRENCE & HAUG LLP

By: 
William S. Frommer
Reg. No. 25,506
(212) 588-0800

"Mark-up" version of Specification

PATENT
450100-3689

#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

TITLE: ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM

INVENTORS: Ryuji Ishiguro
Masafumi Minami

William S. Frommer
Registration No. 25,506
Curtis, Morris & Safford, P.C.
530 Fifth Avenue
New York, New York 10036
(212) 840-3333

ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM

BACKGROUND OF THE INVENTION

1. Field of the Invention:

The present invention relates to an encrypting method and apparatus, a decrypting method and apparatus, and a recording medium in which information encrypted by an encrypting method or an encrypting apparatus is recorded; and more particularly to an encrypting method and apparatus, a decrypting method and apparatus, and a recording medium suitable for use in a system in which information such as video signals, audio signals, data signals or the like is encrypted, the encrypted information is recorded on a recording medium, and the encrypted information is decrypted.

2. Description of the Related Art:

Typically when information is encrypted for recording ~~and then recorded~~ on a ~~predetermined~~ recording medium, the information is encrypted by using a predetermined encryption key, ~~and the encrypted information is recorded on the recording medium.~~ The encrypted information is decrypted by using a decryption key, ~~for decrypting the encrypted information recorded on the recording medium.~~

Two known types of cryptosystems which employ a key (an encryption key) include ~~two cryptosystems;~~ a common-key cryptosystem ~~cryptographic scheme~~ and a public-key cryptosystem. In the common-key cryptosystem, a key (encryption key) used upon encryption is the same as a key

(decryption key) used upon decryption. ~~For example, of the common-key cryptosystems,~~ frequently a data encryption standard (DES) ~~system~~ is ~~frequently~~ employed in common-key cryptosystems. On the other hand, in ~~the~~ public-key cryptosystem, ~~an~~ the encryption key and ~~a~~ the decryption key are different from each other. In this public-key cryptosystem, it is common to open the encryption key ~~is opened~~ to the public, while the decryption key is kept secret. In general, such encryption methods and decryption methods are known.

An encryption method is disclosed in Japanese patent publication No. 60007/1990. According to the method, an encryption key is generated based on a data forming a file to be recorded on a recording medium. Information is encrypted by using the encryption key, and the encrypted information is recorded on the recording medium. The file is reproduced from the recording medium, and a decryption key is generated based on data forming the file. Then, the encrypted information is decrypted by using the generated decryption key.

However, when such encryption ~~method~~ and decryption methods are employed, the file used for generating the encryption key is recorded on one portion (sequent regions) of the recording medium, which may allow the file to be duplicated with comparative ease.

SUMMARY OF THE INVENTION

In view of ~~such aspect~~ the foregoing, it is an object of the present invention to provide encryption method and apparatus, a recording method, and a decryption method and apparatus which provide robust copy protection ~~allows strong copy protect to be effected on the information~~

It is a further object of the invention to provide ~~recorded on a recording medium, and~~ a recording medium where information encrypted by the encrypting apparatus is may be recorded.

According to a first aspect of the present invention, when information to be recorded is encrypted by using an encryption key, an the encryption key is generated ~~based~~ on the basis of ~~inherent~~ information inherent in a recording medium ~~is generated~~ and the information to be recorded on the recording medium is encrypted based on the encryption key. The ~~inherent~~ information inherent in the recording medium may be information from one or more predetermined areas of the medium. ~~is a specific information on a disk.~~

According to a second aspect of the present invention, an encrypting apparatus for encrypting information to be recorded by using an encryption key includes a means for generating an encryption key based on inherent information inherent in a recording medium, and a means for encrypting the information to be recorded on the recording medium based on the encryption key. The ~~inherent~~ information inherent in the recording medium may be information from one or more predetermined areas of the medium. ~~is a specific information on a disk.~~

According to a third aspect of the present invention, when information obtained by encrypting information to be recorded by using an encryption key is recorded on a recording medium, an the encrypted information is ~~received~~ generated according to based on an encryption key, which is in turn generated ~~based on~~ according to ~~inherent~~ information inherent in a the recording medium. ~~The received encrypted information~~ is ~~recorded on a recording medium~~. The ~~inherent~~ information inherent in the recording medium may be information from one or more predetermined areas of the medium ~~is a specific information on a disk.~~

According to a fourth aspect of the present

invention, when an encrypted information recorded on a recording medium is decrypted, there are reproduced from a recording medium a first file storing information encrypted ~~by using~~ an encryption key generated ~~based on a~~ random data ~~to be~~ inserted into a predetermined portion of the encrypted information ~~to be recorded on a recording medium~~, and a second file storing data indicative of ~~a predetermined~~ portion of the random data ~~to be~~ inserted into ~~a predetermined portion of~~ the encrypted information. The random data is detected from the encrypted information stored in the reproduced first file based on the data stored in the reproduced second file ~~and indicating the predetermined portion of the random data~~. A decryption key is generated from the detected random data. The encrypted information of the reproduced first file is decrypted by using the decryption key.

According to a fifth aspect of the present invention, a decrypting apparatus for decrypting an encrypted information recorded on a recording medium includes a means for reproducing from the recording medium a first file storing information encrypted ~~by using~~ an encryption key generated ~~based on a~~ random data ~~to be~~ inserted into a predetermined portion of the encrypted information ~~to be recorded on a recording medium~~ and a second file storing data indicative of ~~a predetermined~~ portion of the random data ~~to be~~ inserted into ~~a predetermined portion of~~ the encrypted information, a means for detecting the random data from the encrypted information stored in the reproduced first file based on the data stored in the reproduced second

file ~~and indicating the predetermined portion of the random~~ data, a means for generating a decryption key from the detected random data, and a means for decrypting the encrypted information of the reproduced first file by using the decryption key.

According to a sixth aspect of the present invention, a recording medium capable of ~~being used in decryption by~~ use in a decrypting apparatus includes a recorded signal capable of being decrypted by the decrypting apparatus. The recorded signal includes a first file storing information encrypted by using an encryption key generated ~~based on~~ on the basis of that is random data ~~to be~~ inserted into one or more predetermined portions of an the encrypted information.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing ~~an arrangement of~~ an encrypting apparatus and a decrypting apparatus according to a first embodiment of the present invention;

FIG. 2 is a diagram showing a logical file format according to the ISO9660 standard;

FIG. 3 is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the first embodiment of the present invention;

FIG. 4 is a table showing an example of an arrangement of a digest method file;

FIG. 5 is a diagram used to explain ~~a method of producing a disk digest~~ the significance of the digest method file entries;

FIG. 6 is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the first

embodiment of the present invention;

FIG. 7 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a second embodiment of the present invention;

FIG. 8 is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the second embodiment of the present invention;

FIG. 9 is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the second embodiment of the present invention;

FIG. 10 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a third embodiment of the present invention;

FIG. 11 is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the third embodiment of the present invention;

FIG. 12 is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the third embodiment of the present invention;

FIG. 13 is a diagram used to explain encrypting and decrypting methods employed by the encrypting and decrypting apparatus according to the third embodiment;

FIG. 14 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a fourth embodiment of the present invention; and

FIG. 15 is a cross-sectional view ~~showing~~ of a disk recording medium ~~having an inherent information recorded on its surface.~~ in accordance with the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

An embodiment of the present invention will hereinafter be described with reference to the accompanying drawings. ~~Informations used in this embodiment are~~ video informations, audio informations, text informations and so on. ~~In this embodiment,~~ recording media ~~on which encrypted information to be decrypted is recorded are,~~ for example, disk-like recording media such as digital video disks (DVD), optical disks, magneto-optical disks, magnetic disks such as flexible disks or hard disks, and so on, and tape-like recording media such as magnetic tapes or the like.

These recording media ~~are slave recording media a large number of which are produced by~~ duplication of a master disk, a master magnetic tape or the like. Data (plain text) to be encrypted is data subjected to the scrambling, the shuffling, the encoding ~~according~~ to moving picture experts group (MPEG) system, ~~the encoding according to~~ joint photographic experts group (JPEG) system and so on. In accordance with the data to be encrypted, data (plain text) decrypted from encrypted data is data ~~to be subjected to the~~ de-scrambling, the de-shuffling, the decoding according to the MPEG system, ~~the decoding according~~ to ~~the~~ JPEG system and so on.

FIG. 1 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to the first embodiment of the present invention, by way of example.

An encrypting apparatus 1 includes ~~an information~~

data generating unit 2 which is formed of a reproducing apparatus for reproducing an information data (such as digital video ~~information~~ data, digital audio ~~information~~ data or the like) from a recording ~~tape and so on on which the information data is recorded~~ medium. The data generating unit 2 outputs the reproduced ~~information~~ data (e.g. plain text) to an encrypting unit 3. The encrypting unit 3 encrypts the ~~information~~ data output from the information data generating unit 2 and outputs an encrypted information data (i.e. a cryptogram) to a recording unit 7 which will be described later on.

The encrypting apparatus also includes an inherent information generating unit 5. ~~which~~ The inherent information generating unit outputs information inherent in a recording medium ~~to the recording unit 7~~ to the recording unit 7 which, for purposes of describing the invention, will be considered ~~A random data~~ For example, random number data ~~or the like is~~ may be employed as the information inherent in the recording medium ~~The~~ in which case the random number data is recorded by the recording unit 7 on a predetermined region of the recording medium ~~such as~~ (e.g. a disk) ~~or the like~~ as a normal file as shown in FIG. 2. Indeed, since the random data is in the form of a normal file, the random data can be copied. But, when this file is copied to the recording medium, such as a hard disk or the like, as shown in FIG. 2, the position (allocation) of this file is changed, which ~~prevents the same information as that of an original disk from being obtained~~ means that a duplicate of an original medium (e.g. read-only disk), having the normal file in the same position as the original, can not be created.

FIG. 2 is a diagram showing a logical file format according to the ISO9660 standard. As shown in FIG. 2, sectors 0 to 149 are set as a pre gap area where data may or may not be recorded. Sectors 150 to 165 are set as a system area where, for example,

copyright information is stored, ~~for example~~. Subsequent sectors 166 to n-1 (were n is ~~a variable number and a predetermined~~ integer ~~value~~) are set as volume descriptors where management informations are stored.

The volume descriptors include a primary volume descriptor where a table of directories (path table) and so on are stored. Sector n and succeeding sectors are user-accessible areas where predetermined files are stored. Each of the sectors is formed of 2 kbytes, and an offset is used to indicate a position therein.

As shown in FIG. 2, for example, the random data can be recorded as an interleaved file. Moreover, the random data can be recorded as a multi extent file. The interleaved file is a file of the random data recorded on a plurality of discontinuous portions in a predetermined area. The multi extent file is a file of the random data which are recorded on a plurality of discontinuous areas as one file.

When the random data is recorded as the interleaved file or the multi extent file, the random data can be recorded on dispersed positions, which makes it more difficult to match the position of the random data recorded on the read-only disk with the position of the random data obtained by copying the random data from the read-only disk.

Moreover, it is possible to record the random data on the pre gap area (00:00:00:00 to 00:00:02:00) or on the system area (00:00:02:00 to 00:00:02:16) according to the ISO9660 standard. When the random data is recorded on either of the

above areas, the recorded random data cannot be accessed as ~~the~~ a normal file, which makes it difficult to copy the random data.

Moreover, it is possible to record the random data ~~on~~ in an application area ~~with its offset within the range from 884th byte to 1395th byte~~ which is located in bytes 884-1395 of the primary volume descriptor area. ~~of the volume descriptor according to the ISO9660 standard. Since this~~ the ISO9660 standard specifies that the application area stores ~~a~~ header information, ~~of the files according to the ISO9660 standard,~~ therefore the random data is recorded ~~on~~ in this ~~the~~ area it cannot be accessed as ~~the~~ a normal file, which makes it difficult to copy ~~the random data stored therein~~.

The random data is finally recorded on a master disk 12 as shown in FIG. 1.

The encrypting apparatus 1 includes a file forming unit 6 for forming a file (digest method file) indicative of a predetermined portion of data on a recording medium. ~~an encrypted information data. Specifically,~~ More particularly, the file forming unit 6 specifies sector numbers and/or offsets ~~designates the random data from a predetermined byte number to another predetermined byte number in the same sector or over different sectors of the random data recorded on the master disk 12 with being inserted in the above encrypted information data.~~ which indicate locations of the inherent information (e.g. random data) within the data (encrypted data + random data) that is recorded on the recording medium. Then, the file forming unit 6 forms a file (digest method file) formed of one or plural pairs of sector numbers and offsets (byte number in a sector). The file indicative of a predetermined portion of the encrypted and random ~~information~~ data (the digest method file) is inserted into ~~an~~ a predetermined area on ~~in the encrypted information data and finally recorded on the~~ master disk 12 such that the master disk contains the encrypted data, the random data, and the digest method file.

The encrypting apparatus 1 includes the recording

unit 7 for recording on a hard disk 8 the random data supplied from the inherent information generating unit 5, the digest method file supplied from the file forming unit 6, and the encrypted information data supplied from the encrypting unit 3. The encrypting apparatus 1 includes a reproducing unit 9 formed of a magnetic head, an amplifier and so on. The reproducing unit 9 reads out the random data from the hard disk 8 based on the digest method file recorded on the hard disk 8 and supplies the read random data to the encryption key generating unit 4. The reproducing unit 9 also reads out the encrypted information data and supplies the encrypted information data together with the random data and the digest method file to a formatting unit 10.

The formatting unit 10 formats the encrypted information data and the digest method file supplied from the reproducing unit 9 to produce a pre-master image. The formatting unit 10 supplies the pre-master image to the recording unit 7. At this time, as described above, the formatting unit 10 can format the random data as the normal file according to the ISO9660 standard, and, as described above, can format the data as the interleaved file or the multi extent file. The recording unit 7 records the pre-master image on the hard disk 8. The encrypting apparatus 1 includes a recording unit 11 formed of an optical head, an amplifier and so on. The recording unit 11 records the pre-master image reproduced from the hard disk 8 by the reproducing unit 9 on the master disk 12. A disk producing apparatus 13 employs the master disk 12 as an

original disk to reproduce a large number of disks 15 (slave disks).

A decrypting apparatus 14 includes a reproducing unit 16, a decrypting unit 17, a decryption-key generating unit 18, and an output terminal 19. The reproducing unit 16 reproduces the disk 15. The decryption-key generating unit 18 generates a decryption key based on a reproduced signal supplied from the reproducing unit 16, and outputs the decryption key to the decrypting unit 17 which will be described later on. The decrypting unit 17 decrypts the reproduced signal supplied from the reproducing unit 16 based on the decryption key supplied from the decryption-key generating unit 18.

An encrypting operation of the encrypting apparatus 1 will be described with reference to FIG. 3 which is a flowchart therefor. In step S1, initially, the inherent information generating unit 5 generates the random data (random-number data) which is ~~a value (encryption key)~~ inherent in recording medium and supplies the random data to the recording unit 7. In this step, the file forming unit 6 determines from which area of the master disk 12 the random data (random-number data) used ~~for the value (encryption key)~~ inherent in the recording medium is extracted, and then produces a file (digest method file) indicative ~~of one or a plurality~~ of determined areas.

As shown in FIG. 4, for example, the digest method file is formed of a table including a large number of offsets (offset numbers) of n sectors from the sector number 1 to the sector number n (where n is the number of about several tens).

As shown in FIG. 5, the table designates data ~~from a predetermined offset in a sector of the sector number 1 to another predetermined offset therein and data from a predetermined offset in a sector of the sector number 2 to another predetermined offset therein.~~ by referring to sectors and offsets within those sectors The digest method file is recorded by the recording unit 7 on the hard disk 8. The random data is also recorded by the recording unit 7 on the hard disk 8.

The processing proceeds to step S2. The reproducing unit 9 reproduces the random data ~~of~~ according to the digest method file, which is determined in step S1 and recorded on the hard disk 8, ~~from the predetermined offset in the sector of the sector number 1 to another predetermined sector therein and from the predetermined offset in the sector of the sector number 2 to another predetermined offset therein.~~ by retrieving the data specified by the sector numbers and offsets contained in the digest method file. The reproducing unit 9 then gathers the reproduced random data. The reproducing apparatus 9 supplies these gathered random data to the encryption-key generating unit 4.

In step S3, the encryption-key generating unit 4 subjects the random data supplied from the reproducing unit 9 to a predetermined calculation (e.g., addition) or generates the encryption key (inherent value, disk digest) from the random data itself as shown in FIG. 5. Then, the processing proceeds to step S4. In step S4, the encryption-key generating unit 4 supplies the generated encryption key to the encrypting unit 3. The encrypting unit 3 encrypts the information data supplied from the information data generating unit 2 based on the

supplied encryption key. The encrypting unit 3 supplies the encrypted information data to the recording unit 7. Then, the recording unit 7 records the encrypted information data on the hard disk 8.

Then, the processing proceeds to step S5. the reproducing unit 9 reproduces the recorded encrypted information data, the random data which is to be the information inherent in the recording medium, and the digest method file indicative of the predetermined portion of the encrypted information data where the random data is ~~which~~ are recorded on the hard disk 8, and supplies them to the formatting unit 10. The formatting unit 10 then generates the pre-master image (format signal) from the encrypted information data, the random data ~~which is to be the information inherent in the recording medium~~, and the digest ~~file~~ method file ~~indicative of the predetermined portion of the encrypted information data all of that are supplied from the reproducing unit 9.~~ At this time, as described above, the formatting unit 10 formats the random data as a normal file according to the ISO9660 standard. Moreover, the formatting unit 10 can format the random data as an interleaved file or a multi extent file to be dispersed.

The formatting unit 10 supplies the produced pre-master image to the recording unit 7. The recording unit 7 temporarily records the pre-master image on the hard disk 8. The reproducing unit 9 reproduces the pre-master image recorded on the hard disk 8 and supplies the reproduced data to the recording unit 11. The recording unit 11 records the reproduced

data supplied from the reproducing unit 9 on the master disk 12. Alternatively, the formatting unit 10 can supply the pre-master image, i.e., the formatting signal directly to the recording unit 11 which records the pre-master image on the master disk 12.

The disk producing apparatus 13 employs the master disk thus produced as an original disk to reproduce a large number of the disks (slave disks such as a DVD, an optical disk, a magneto-optical disk, or the like) 15. When the magnetic tape is employed as the recording medium, a transfer apparatus may be employed to transfer signals recorded on ~~the~~ a master magnetic tape to a large number of slave magnetic tapes.

A decrypting operation of the decrypting apparatus 14 will be described with reference to FIG. 6 which is a flowchart therefor. In step S11, the reproducing unit 16 reproduces the signals recorded on the disk 15. The reproducing unit 16 supplies the reproduced signal to the decrypting unit 17 and, when the decryption-key generating unit 18 supplies a gate signal to the reproducing unit 16, also supplies a file of the recorded signal where the random data is stored and the digest method file to the decryption-key generating unit 18.

The processing proceeds to step S12. In step S12, the decryption-key generating unit 18 extracts from the random data supplied from the reproducing unit 16 the random data designated by the digest method file~~, e.g., the random data from the predetermined offset to another predetermined offset in the sector of the sector number 1 and the random data from the~~

predetermined offset to another predetermined offset in the sector of the seetor number 2, and then gathers the extracted random data.

Then, the processing proceeds to step S13. In step S13, the decryption-key generating unit 18 generates the decryption key corresponding to the original encryption key from the random data gathered in step S12 and subjected to the predetermined calculation (e.g., addition), or from the random data itself. The decryption-key generating unit 18 supplies the generated decryption key to the decrypting unit 17. Then, the processing proceeds to step S14. In step S14, the decrypting unit 17 decrypts the reproduced data supplied from the reproducing unit 16, i.e., the encrypted information data (cryptogram) based on the decryption key supplied from the decryption-key generating unit 18, thus obtaining the original information data (plain text), e.g. generated by the data generating unit. The decrypting unit 18 outputs the original information data through the output terminal 19.

If the encrypting apparatus 1 records pit strings of the recording signal on the track of the master disk 12 in a wobbled fashion, then the inherent information generating unit 5 may generates a wobbling signal indicative of the wobbling of the pit strings of the recording signal to be recorded on the master disk 12 as the information signal inherent in the recording medium 12. If the information inherent in the disk 15 as the recording medium is a physical information to be formed on the disk 15 and a track on which the recording signal of the master disk 12 is to be recorded is a wobbled pregroove or a

wobbled land portion, the wobbling signal corresponding to the pregroove or the land portion may be generated as the information signal inherent in the recording medium from the inherent information generating unit 5.

The encryption-key generating unit 4 generates an encryption key based on the wobbling signal and supplies the generated encryption key to the encrypting unit 3. The encrypting unit 3 encrypts the information data supplied from the information data generating unit 2 based on the encryption key supplied from the encryption-key generating unit 4.

In this case, the decrypting apparatus 14 is operated as follows. Specifically, the decryption-key generating unit 18 detects a wobbling frequency of the pregroove or the land portion corresponding to the predetermined portion of the recording signal on the disk 15. The decryption-key generating unit 18 generates the decryption key obtained by subjecting the data corresponding to the wobbling frequency to a predetermined calculation or generates the decryption key corresponding to the original encryption key based on the data itself corresponding to the wobbling frequency. The decryption-key generating unit 18 supplies the generated decryption key to the decrypting unit 17. The decrypting unit 17 decrypts the encrypted information data (cryptogram) supplied from the reproducing unit 16 by using the decryption key supplied from the decryption-key generating unit 18, to obtain the original information data (plain text).

As described above, if the information inherent in the recording medium is the physical information to be recorded

on the recording medium, e.g., the wobbled pregroove or the wobbled land portion of the recording medium, then the recording medium may be a disk having a considerable thickness and a comparatively rigid substrate, such as a DVD, an optical disk, a magneto-optical disk, a hard disk or the like.

When the random data is employed as the information inherent in the recording medium and the position where the random data is recorded is managed by the digest method file as described above, ~~it is possible to effect the~~ effective copy ~~protect in the information~~ protection may be realized.

Since the normal file according to the ISO9660 standard is employed, ~~and when the file is duplicated to the recording medium, the file is recorded on a different position of the~~ the position of the file is shifted upon duplication of the file to a recording medium, it is impossible to ~~obtain the same information as that of the original disk~~ create a copy of the medium on which the file is recorded. and therefore. ~~Therefore, it is possible to effect the more effective copy protect on the information.~~

FIG. 7 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus, to which the encrypting and decrypting method according to the present invention is applied, according to a second embodiment of the present invention. An encrypting apparatus 1 shown in FIG. 7 has a random file forming unit 20 instead of the inherent information generating unit 5 of the encrypting apparatus 1 shown in FIG. 1 and also has a file forming unit 21 for forming a file indicative of a predetermined portion of the random file instead of the file forming unit 6 for forming a file indicative

of the predetermined portion of the encrypted information. Other arrangements and operations of the encrypting and decrypting apparatus 1 and 14 shown in FIG. 7 are similar to those of the encrypting and decrypting apparatus 1, 14 shown in FIG. 1 and hence will not be described.

An operation of the encrypting apparatus 1 shown in FIG. 7 will be described with reference to FIG. 8 which is a flowchart therefor. The random file forming unit 20 includes a pseudo random data generator for generating a random data. In step S21, the random file forming unit 20 produces a random file including a random data of, for example, several kbytes or larger generated by the pseudo random data generator. The random file forming unit 20 supplies the random file, for example, to the recording unit 7. The recording unit 7 records the random file on the hard disk 8.

Then, the processing proceeds to step S22. In step S22, the file forming unit 21 determines from which portions of the random file random-number data (random data) used for obtaining an inherent value (encryption key) is gathered, i.e., determines from which portion(s) of the random data the random data is gathered (e.g. from a predetermined sector/offset ~~number~~ to another predetermined sector/offset, ~~number~~ or ~~the random data formed of~~ from a plurality of predetermined non-adjacent portions designated by sectors and/or offsets ~~is gathered~~. The file forming unit 21 forms a digest method file indicative of the ~~predetermined~~ portion(s) of these random data and supplies the digest method file to the recording unit 7. The recording unit 7 once records the digest method file on the hard disk 8. Finally, the reproducing unit 9 reads

out the recorded digest method file from the hard disk 8 and supplies the reproduced digest method file to the recording unit 11, and the recording unit 11 records the digest method file on the master disk 12.

Then, the processing proceeds to step S23. In step S23, the reproducing unit 9 ~~gathers~~ reproduces the random data, recorded on the hard disk 8 ~~of the one predetermined portion from the predetermined offset address to another predetermined offset address or the random data, recorded on the hard disk 8, of a plurality of predetermined portions, and reproduces them.~~ based on the information co The reproducing unit 9 supplies the reproduced random data to the encryption-key generating unit 4. The encryption-key generating unit 4 generates the encryption key (inherent value) (disk digest) from the random data itself or the random data subjected to the predetermined calculation.

Then, the processing proceeds to step S24. In step S24, the position where the random file is allocated in the master disk 12 is calculated, i.e., ~~there is calculated~~ an offset value is calculated and added to the offset(s) specified in the digest method file. ~~(offset number) of a predetermined sector number obtained when the random file is inserted into the encrypted information data recorded on the hard disk 8 and then recorded on the master disk 12. The calculated offset value is added to the offset number (offset value) designated by the digest method file.~~ Thus, the digest method file is modified.

Then, the processing proceeds to step S25. In step S25, the encryption-key generating unit 4 supplies the generated encryption key (the inherent value) (disk digest) to the

encrypting unit 3. The encrypting unit 3 encrypts the information data supplied from the information data generating unit 2 and supplies the encrypted information data to the recording unit 7. The recording unit 7 records the encrypted information data on the hard disk 8.

Then, the processing proceeds to step S26. In step S26, the reproducing unit 9 reproduces the encrypted information data, the signal indicative of the information inherent in the recording medium, and the digest method file ~~indicative of the predetermined encrypted portion from the hard disk 8~~ and supplies them to the formatting unit 10. The formatting unit 10 formats the information data, the information signal and the digest method file to produce the pre-master image. In this formatting operation, as described above, the formatting unit 10 can format the random file as an interleaved file or a multi extent file ~~to disperse the random file to the different positions~~.

The formatting unit 10 supplies the pre-master image to the recording unit 7 and the recording unit 7 ~~once~~ records the pre-master image on the hard disk 8. The reproducing unit 9 then reproduces the pre-master image recorded on the hard disk 8 and supplies the reproduced pre-master image to the recording unit 11. The recording unit 11 records on the master disk 12 either the pre-master image supplied from the reproducing unit 9 or the pre-master image supplied directly from the formatting unit 10.

The disk producing apparatus 13 ~~employs~~ uses the master disk 12 as an original disk for generating ~~to obtain~~ a large number of the

disks (slave disks) 15 by duplication ~~of the master disk 12~~.

A decrypting operation of the decrypting apparatus 14 shown in FIG. 7 will be described with reference to FIG. 9 which is a flowchart therefor. In step S31, the reproducing unit 16 reproduces the disk 15 and supplies the reproduced data to the decryption-key generating unit 18. Then, ~~the processing proceeds to step S32.~~ In step S32, the decryption-key generating unit 18 extracts from the reproduced encrypted information data the random data, designated by the digest method file, ~~of a portion from the predetermined offset to another predetermined offset in the sector of the predetermined sector number and of another portion from the predetermined offset to another predetermined offset. The decryption-key generating unit 18 gathers them.~~

Then, the processing proceeds to step S33. In step S33, the decryption-key generating unit 18 generates the decryption key obtained by subjecting the random data to the predetermined calculation, or the decryption key corresponding to the original encryption key based on the random data itself, and then supplies the generated decryption key to the decrypting unit 17. ~~Then, the processing proceeds to step S34.~~ In step S34, the decrypting unit 17 decrypts the encrypted information data (cryptogram) supplied from the reproducing unit 16 by using the decryption key supplied ~~from the decryption key supplied~~ from the decryption-key generating unit 18 to obtain the original information data (e.g. plain text). The decrypting unit 17 outputs the original information data through the output

terminal 19.

FIG. 10 is a block diagram ~~showing arrangements~~ of an encrypting apparatus and a decrypting apparatus according to a third embodiment of the present invention. The arrangement of the encrypting apparatus 1 shown in FIG. 10 is basically similar to the encrypting apparatus shown in FIG. 1 and hence will not be described.

An encryption method employed by the encrypting apparatus 1 shown in FIG. 10 will be described with reference to FIG. 11 which is a flowchart therefor. In step S41, a distribution key (distribution-key data) to be distributed to a user is ~~properly~~ determined, and is registered in a memory (e.g., a semiconductor memory) in the encryption-key generating unit 4. The distribution key may be registered in a central processing unit (CPU) (which may include the memory) instead of the memory.

Then, the processing proceeds to step S42. In step S42, in a manner similar to that ~~similarly to the processing~~ described ~~above~~ with reference to the flowchart of FIG. 3, the encryption-key generating unit 4 gathers the information inherent in the disk 15 and subjects the information to a predetermined calculation to generate the disk digest (key). ~~Then, the processing proceeds to step S43.~~ In step S43, the encryption-key generating unit 4 subjects the distribution key determined in step S41 and the disk digest generated in step S42 to a predetermined calculation, e.g., exclusive-ORs the distribution key and the disk digest and sets the calculated result as a work key.

The processing proceeds to step S44. In step S44,

the encryption-key generating unit 4 supplies the work key obtained through the calculation in step S43 to the encrypting unit 3 as the encryption key. The encrypting unit 3 encrypts the information data based on the encryption key and supplies the encrypted information data to the recording unit 7. The recording unit 7 records the encrypted information data on the hard disk 8.

The decrypting apparatus 14 shown in FIG. 10 has a key reading unit 22 and a key medium 23, ~~newly~~ provided in addition to those of the decrypting apparatus 14 shown in FIG. 1. The key medium 23 is arranged such that the above-mentioned distribution key can be distributed. For example, the distribution key may be printed on some suitable object in the form of Arabic numerals, symbols, bar codes, other codes similar to the bar codes or the like. The key medium 23 can be ~~formed of~~ a card or the disk 15 itself.

The key medium 23 may includes a memory, such as a semiconductor memory or the like storing the distribution key, or a CPU or the like ~~including the~~ memory. The key medium 23 ~~including the~~ memory or the CPU may be ~~formed of~~ a card (e.g., an integrated circuit (IC) card) or the like. The key medium 23 may be arranged such that the distribution key is recorded thereon magnetically or optically. Such key medium 23 ~~is to~~ be sold ~~on a market solely~~ or together with a reproducing apparatus for reproducing the disk 15. The key reading unit 22 reads out the distribution key printed on or recorded on the key medium 23.

A decrypting operation of the decrypting apparatus 14 shown in FIG. 10 will be described with reference to FIG. 12 which is a flowchart therefor. In step S51, the key reading unit 22 reads out the distribution key printed on or recorded on the key medium 23 and supplies the distribution key to the decryption-key generating unit 18. Then, the processing proceeds to step S52. In step S52, ~~similarly to the processing decryption processing~~ in a manner similar to that described with reference to FIG. 6, the decryption-key generating unit 18 gathers the information inherent in the disk 15 and subjects the information to a predetermined calculation, thereby obtaining the disk digest (key) corresponding to the original disk digest (key).

Then, the processing proceeds to step S53. In step S53, the decryption-key generating unit 18 subjects the distribution key obtained in step S51 and the disk digest obtained in step S52 to a predetermined calculation, e.g., exclusive-ORs the distribution key and the disk digest, thereby obtaining the work key. ~~Then, the processing proceeds to step S54.~~ In step S54, the decryption-key generating unit 18 supplies the work key obtained in step S53 ~~as the decryption key~~ for use as the decryption key to the decrypting unit 17. The decrypting ~~key~~ unit 17 decrypts the encrypted information data supplied from the reproducing unit 16 by using the decryption key supplied from the decryption-key generating unit 18 and then outputs the decrypted information data through the output terminal 19.

FIG. 13 is a diagram used to explain the encryption method and the ~~description~~ decryption method respectively employed in the

encrypting apparatus 1 and the decrypting apparatus 14 shown in FIG. 10. ~~Specifically~~ Initially, the plain text (e.g. data) is encrypted based on the distribution key and the disk digest, and the resulting cryptogram ~~obtained by encryption of the plain text~~ is recorded on the disk. The distribution key is supplied to a user through a route other than the disk. The cryptogram read out from the disk is decrypted based on a key that is derived by operating on the disk digest ~~obtained by calculation of the~~ and distribution key ~~and the data read out from predetermined one or plural areas of the disk. Thus, the decrypted plain text is output.~~

FIG. 14 is a block diagram showing an encrypting apparatus and a decrypting apparatus according to a fourth embodiment of the present invention.

An encrypting apparatus 1 shown in FIG. 14 has a random file forming unit 20 and a random file forming unit 21 for forming a file indicative of a predetermined portion of the random file, both similar to those shown in FIG. 7 ~~instead of~~ and replacing the inherent information generating unit 5 and the file forming unit 6 of the encrypting apparatus 1 shown in FIG. 10. The random file forming unit 20 and the file forming unit 21 are operated ~~basically similarly to those~~ in a manner similar to the corresponding elements described with reference to FIG. 7, ~~and~~ the other units of Fig. 14 are ~~also~~ operated ~~basically similarly to the those~~ in a manner similar to the corresponding elements described with reference to FIG. 10. Therefore, the operations of the encrypting apparatus 1 and the decrypting apparatus 14 shown in FIG. 14 will not be described. The encrypting apparatus 1 and the decrypting apparatus 14 of Fig. 14 ~~having such arrangements~~ can carry out the operations of encrypting ~~the~~

data (e.g. plain text) plain ~~text~~ and decrypting the cryptogam resulting ~~obtained by encryption of the plain text~~ by the method shown in FIG. 13.

Regardless employed (first, second, third, fourth embodiment) ~~Even if any~~ of the encrypting apparatus 1 ~~according to the first to fourth embodiments is employed to read~~ the information data (file) ~~from the predetermined recording medium (the disk 15 in this case) and to dub (or copy) the information~~ data on another ~~predetermined medium, then it~~ is impossible to ~~obtain the same data as recorded on the~~ make a copy of data from original recording medium from to another recording medium, because the ~~information~~ position of the data is shifted during the dubbing process, ~~data is usually recorded on another recording medium at the positions different from those where the information data is recorded on the original recording medium.~~ Therefore, it is impossible to decrypt the encrypted ~~information~~ data from the dubbed medium. ~~Alternatively~~, Moreover, even if ~~the information~~ data recorded on the dubbed ~~another recording~~ medium can be decrypted, it is impossible to output the decrypted information data through the output terminal as the digital signals. As a result, ~~employment~~ use of the encrypting apparatus and method of the present invention makes it difficult to copy the information data on an original recording medium to another recording medium.

~~Since~~ When the random file is arranged as an interleaved file or the multi extent file ~~and hence recorded on the different and dispersed positions of the recording medium, as described above,~~ it ~~becomes~~ is even more difficult to match the position(s) of the random data recorded on the ~~read only~~ original disk with the positions of the random data copied on the ~~on the hard~~ disk ~~from the read-only disk.~~ Therefore, the illegitimate dubbing ~~copying~~ can be ~~suppressed~~ prevented.

In each of the first to fourth embodiments, as shown in FIG. 15, the information inherent in the disk 15 can be recorded by ultraviolet laser or the like on a disk surface, i.e., a surface of the disk substrate 33.

When the information inherent in the disk which is recorded on the surface of the disk substrate 33 is read out, rays of light must be condensed directed on the surface of the disk substrate 33 by moving an optical head (not shown) in the direction perpendicular to the disk surface ,and further a special reading apparatus and a special reading command (e.g., a command to move the optical head in the direction perpendicular to the disk surface) are required. Therefore, it becomes difficult to read the information thus recorded, and it becomes impossible to easily copy such information.

This arrangement ~~can also be~~ is effective in protecting the information from an optical ~~copy or a~~ copying and so-called "peel and copy". ~~The~~ Copying by "peel and copy" ~~is to~~ refers to physically ~~copy~~ copying pits 32 formed on the disk substrate 33 after a protective film 31 is peeled off from the disk substrate 33. ~~Specifically, the information inherent in the disk is recorded or printed on the disk substrate 33, it is possible to protect the information inherent in the disk from the "peel and copy" and the optical copy in which rays of light are irradiated on the pits 32 of the disk substrate 33 and the copy is carried out based on the reflected light or the transmission light.~~

Optical copying refers to radiating the pits 32 of the disk substrate 33 and copying the pit arrangement on the basis of the reflected light.

The apparatus and methods according to the first to fourth embodiments of the present invention can be used in ~~utilized for~~

communication, such as wire communication (e.g., communication through an electric cable, an optical fiber cable or the like), wireless communication (communication utilizing electric waves, light, sound waves or the like), or the like. In ~~this case~~ these cases, the encrypting apparatus 1 supplies the cryptogram to the decrypting apparatus 14 through the wire communication or the wireless communication.

While the file is formatted in accordance with the ISO9660 standard in the first to fourth embodiments, the present invention is not limited thereto. While the work key is generated by ~~calculating~~ operating on the distribution key and the disk digest ~~in the first to fourth embodiments~~, the present invention is not limited thereto. The work key may be generated by, for example, ~~calculating~~ operating on the distribution key and the wobbling signal.

According to the encrypting apparatus and method of the present invention, since the information inherent in the recording medium is may be set as the frequency of the predetermined portion(s) of the wobbled pregroove or the wobbled land ~~portion to be formed on the recording medium~~, it is possible to ~~effect the~~ realize strong copy protection of recorded information.

According to the encrypting apparatus and method of the present invention, since the information inherent in the recording medium is may be set as the random data to be inserted into ~~the~~ predetermined portion(s) of the encrypted information to be recorded on the recording medium, ~~dispersion of~~ and insertion positions of the random-data may be dispersed, ~~insertion positions can make~~ making it difficult to read the random data. Thereby, providing strong copy protection of the recorded information. ~~and it is possible to effect the strong copy protect on the~~

~~information.~~

According to the encrypting method of the present invention, since ~~the third encryption~~ a work key ~~is~~ may be generated from ~~the first~~ a disk digest key (generated from the information inherent in the recording medium) and ~~the second key~~ a distribution key (independent of the ~~first~~ work key), and the information to be recorded on the recording medium is encrypted by using the ~~third~~ work key, ~~it is possible to simplify the arrangement of the encrypting apparatus and it is possible to effect the strong copy protect on the information.~~ effective copy protection of recorded information is provided.

According to the decrypting apparatus and method of the present invention, the encryption key is generated based on the random data to be inserted into the predetermined portion(s) of the encrypted information to be recorded on the recording medium. By using the encryption key, the first file and the second file are ~~respectively~~ reproduced from the ~~first~~ file ~~where the encrypted information is stored and the~~ recording medium ~~where the second file in which there is recorded the data indicative of the predetermined portion of the random data to be inserted into the predetermined portion of the encrypted information.~~ The data stored in the first file includes encrypted data and random data. ~~Based on~~ the data stored in the reproduced second file ~~and indicating~~ indicates predetermined portion(s) of the ~~random data, the random data is detected from the encrypted information stored in~~ where the random data is located the first file. The decryption key is generated from the detected random data and the encrypted information data of the reproduced first file is decrypted by using the decryption key. ~~Therefore, it is possible to decrypt the information protected by the strong copy protect.~~

According to the decrypting method of the present invention, the encryption key is generated based on the wobbling frequency of the predetermined portion of the encrypted information to be recorded on the recording medium. By using the encryption key, the first file and the second file are respectively reproduced from the first file where the encrypted information is stored and the recording medium where the second file in which there is recorded the data indicative of the predetermined portion of the predetermined portion of the encrypted information to be recorded on the recording medium. Based on the data stored in the reproduced second file and indicating a predetermined portion of the encrypted information, the wobbling frequency of the predetermined portion of the encrypted information is detected. The decryption key is generated based on the detected wobbling frequency. The encrypted information of the reproduced first file is decrypted by using the decryption key. Therefore, it is possible to decrypt the information protected by the strong copy protect.

According to the decrypting method of the present invention, the encryption key is generated based on the frequency of the predetermined portion of the wobbled pregroove or the wobbled land portion to be formed on the recording medium. By using the encryption key, the first file and the second file are respectively reproduced from the first file where the encrypted information is stored and the recording medium, where the second file in which there is recorded the data indicative of the predetermined portion of the wobbled pregroove

and/or the wobble land portion to be formed on the recording medium.

Based on the data stored in the reproduced second file ~~and indicating predetermined portion of the wobbled pregroove or the wobbled land portion~~, the wobbling frequency of the predetermined portion(s) of the pregroove or the land portion ~~formed on the recording medium~~ is detected. The decryption key is generated based on the detected wobbling frequency, and the encrypted information of the reproduced first file is decrypted by using the decryption key. ~~Therefore, it is possible to decrypt the information protected by the strong copy protect.~~

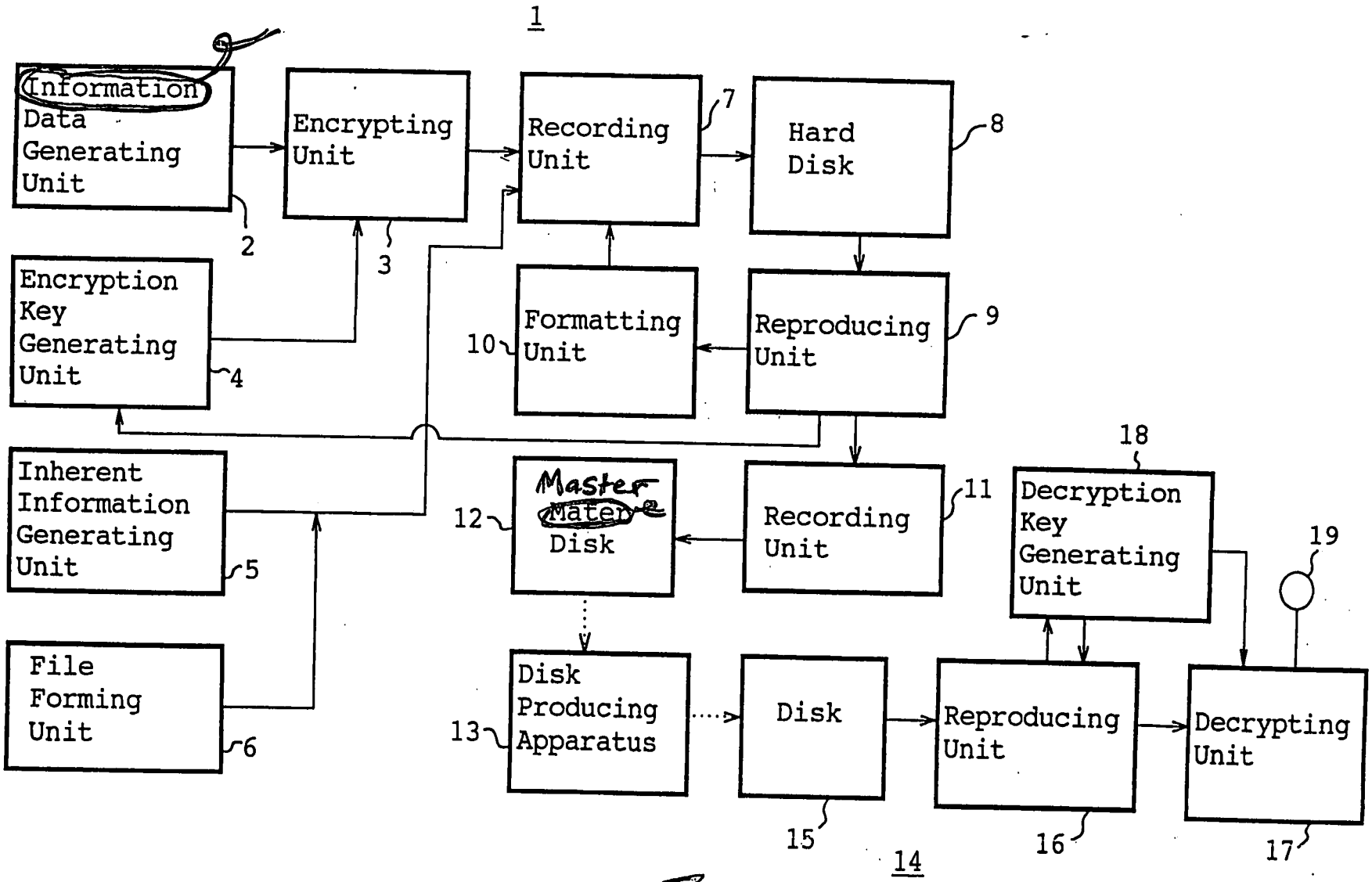
According to the decrypting method of the present invention, the encryption key is generated based on the random data selected from the predetermined portion(s) of a random file formed of random data generated by ~~the predetermined~~ pseudo random data generator. The file storing the information encrypted by using the encryption key, the file storing the data indicative of the predetermined portion(s) of the random file, ~~formed of the random data~~ and the random file are reproduced. Based on the file storing the data indicative of the predetermined portion(s) of the reproduced random file, the decryption key is generated ~~from the~~ (i.e. generated according to the random data at the portions ~~of~~ indicated by the random file). By using the decryption key, the ~~encryption~~ encrypted information reproduced from the recording medium is decrypted. ~~It is possible to decrypt the information protected by the strong copy protect.~~

According to the decrypting method of the present invention, decryption is performed a work by using ~~the third~~ key generated from a disk ~~the first~~ that is

~~encryption key~~ digest generated from the information inherent in the recording medium and ~~the second~~ a distribution key independent of the ~~first~~ disk digest encryption key ~~the information is encrypted.~~ The ~~first decryption key~~ disk digest is generated from the information inherent in the recording medium where the encrypted information is recorded. The ~~third decryption~~ work key is generated based on the ~~first decryption key~~ disk digest and ~~the second decryption~~ distribution key recorded on the predetermined key medium ~~and corresponding to the second encryption key.~~ By using the ~~third decryption~~ work key, the information encrypted by using the ~~third encryption~~ work key and reproduced from the recording medium is decrypted. ~~It is possible to decrypt the information protected by the strong copy protect.~~

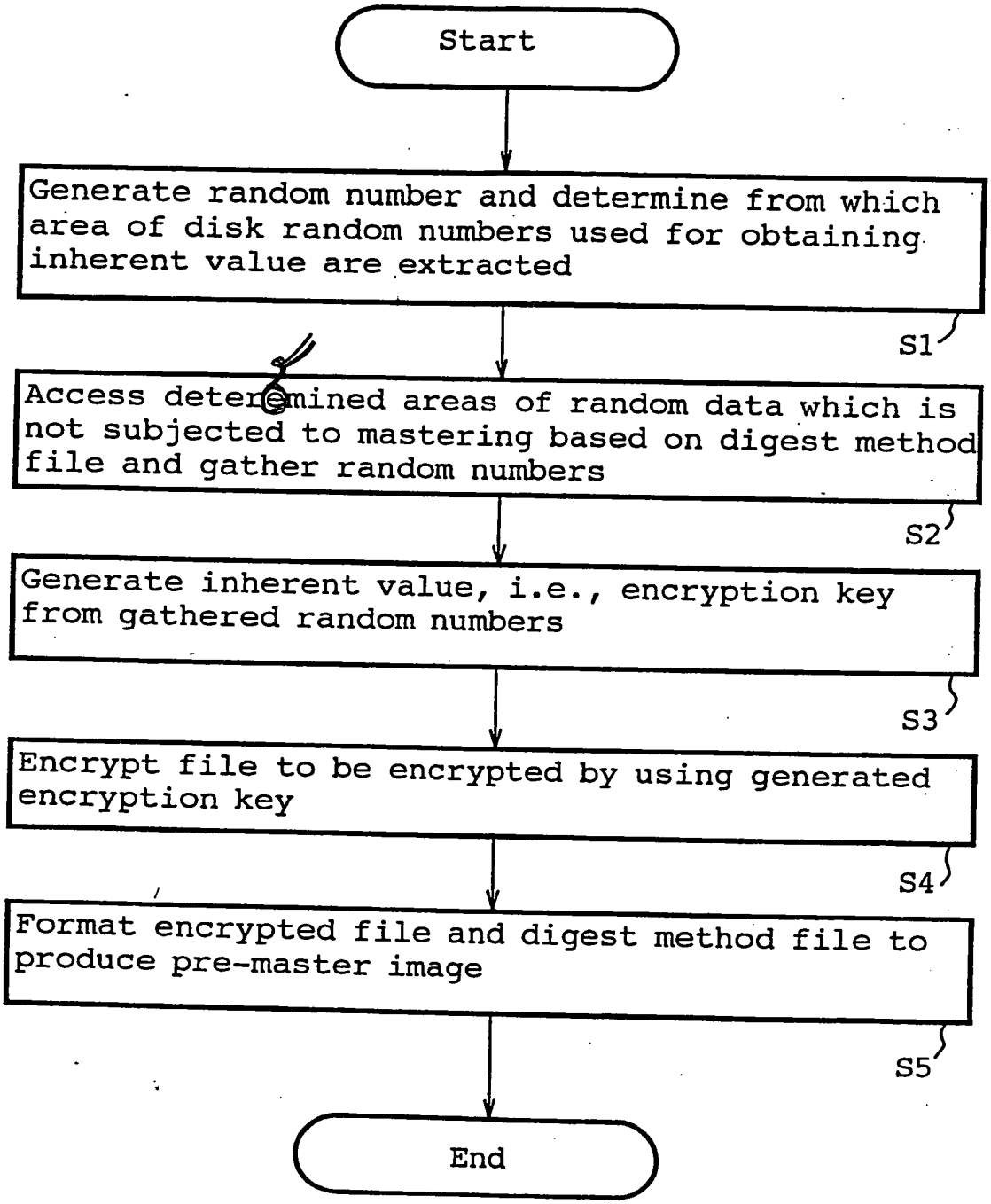
Having described preferred embodiments of the present invention with reference to the accompanying drawings, it is to be understood that the present invention is not limited to the above-mentioned embodiments and that various changes and modifications can be effected therein by one skilled in the art without departing from the spirit or scope of the present invention as defined in the appended claims.

FIG. 1



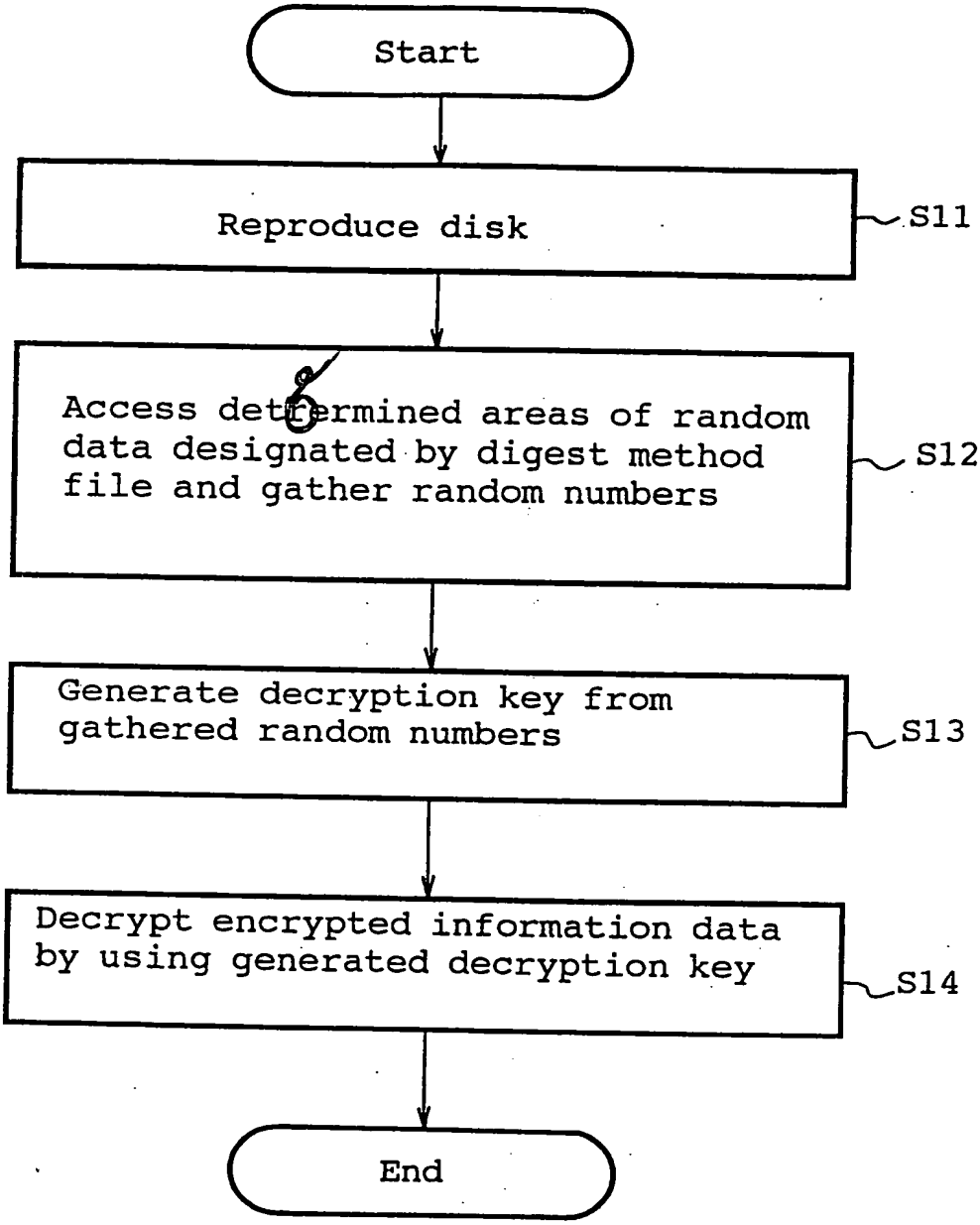
Approved 24 Oct 2003 JWS

FIG. 3



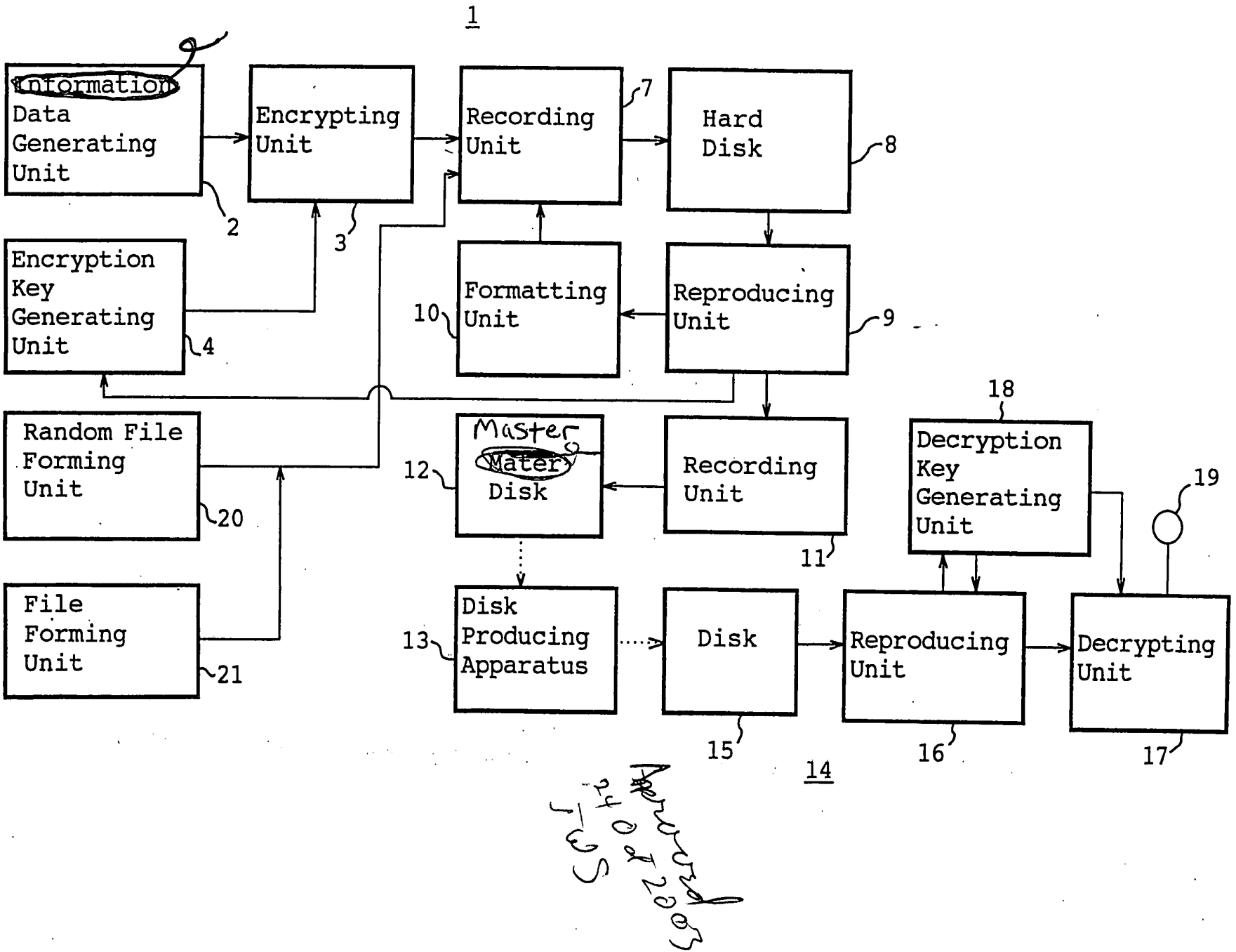
Approved
24 Oct
2003
JWS

FIG. 6



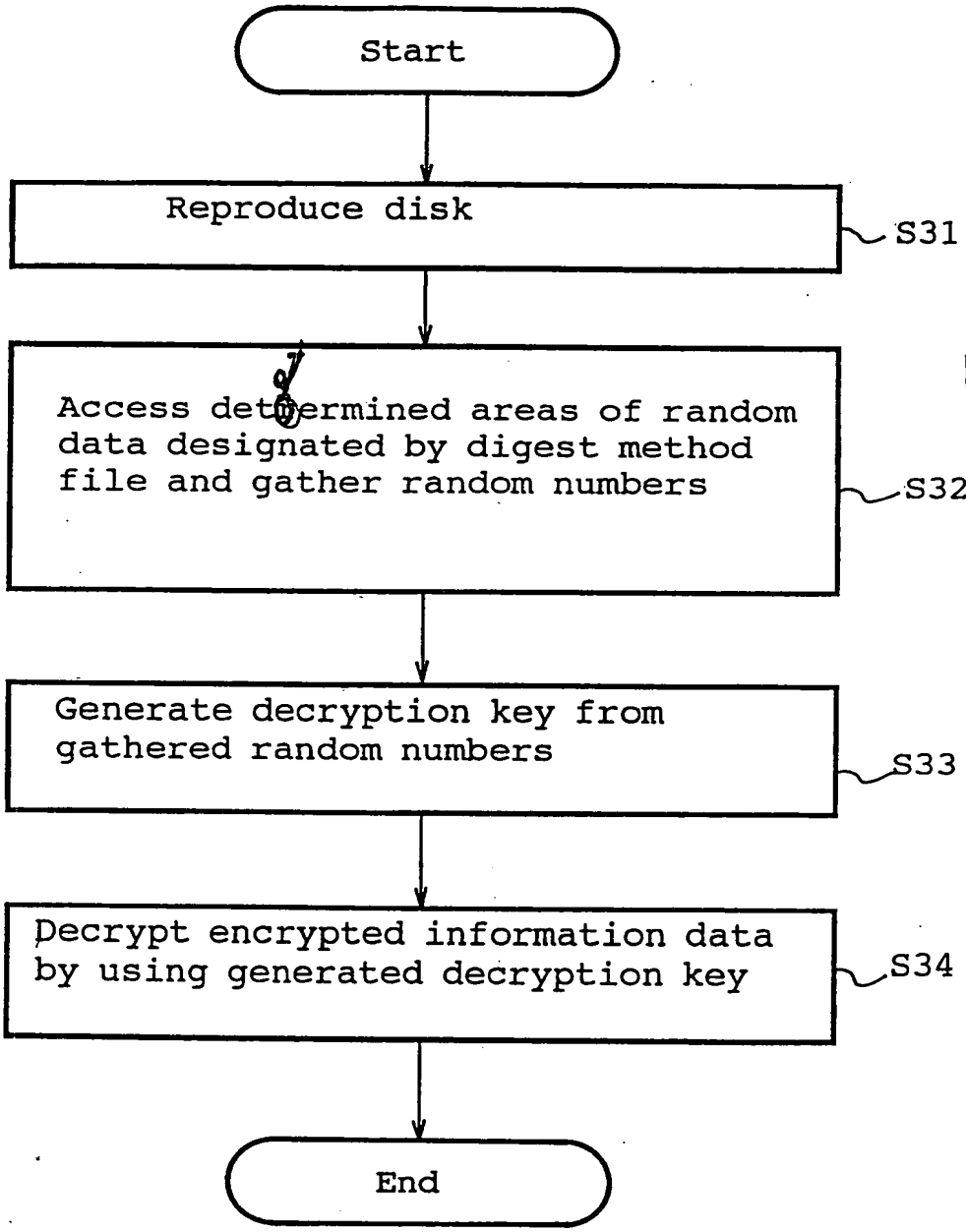
Approved 24 Oct 2003 JWS

FIG. 7



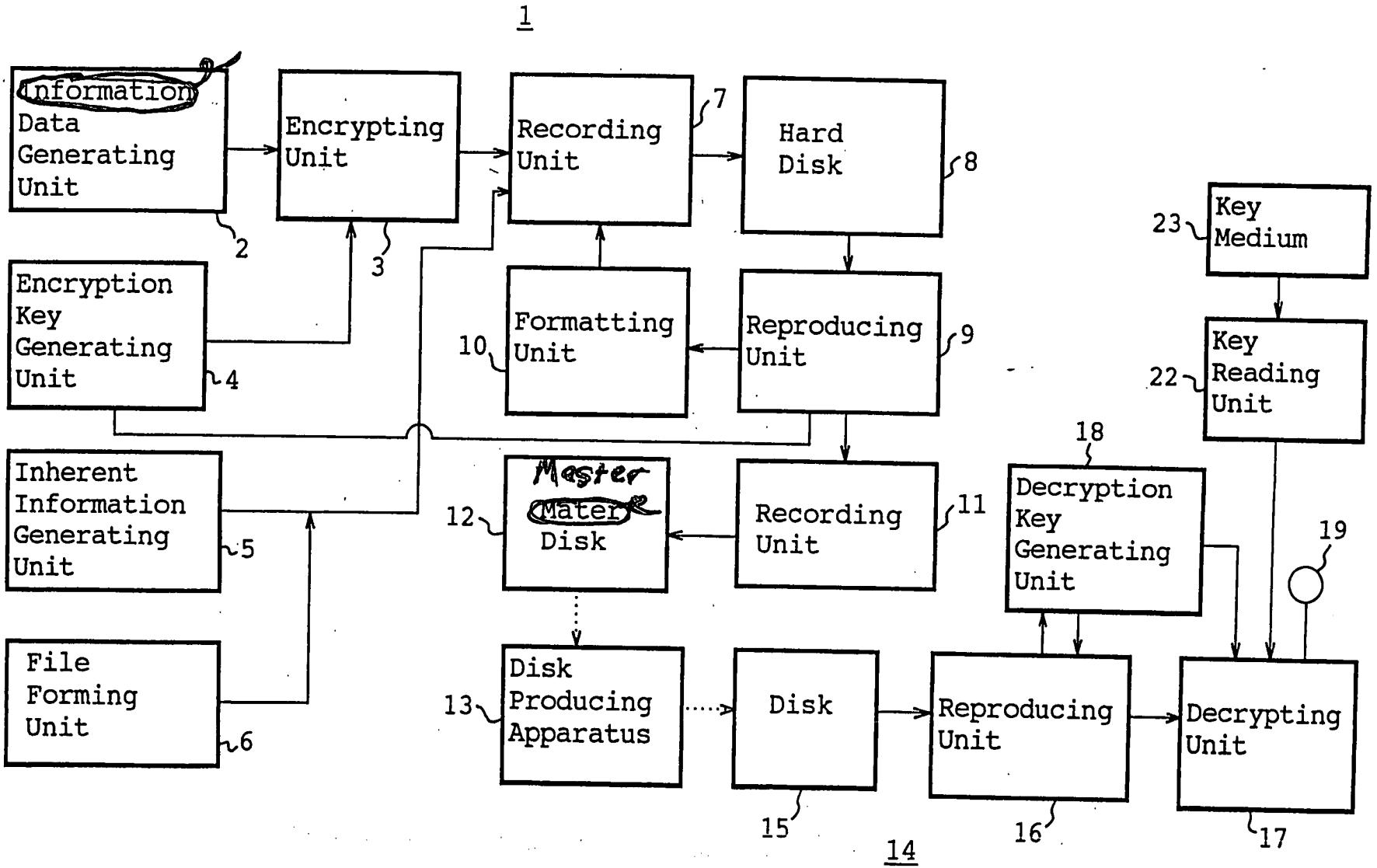
Approved
24 Oct 2003
JWS

FIG. 9



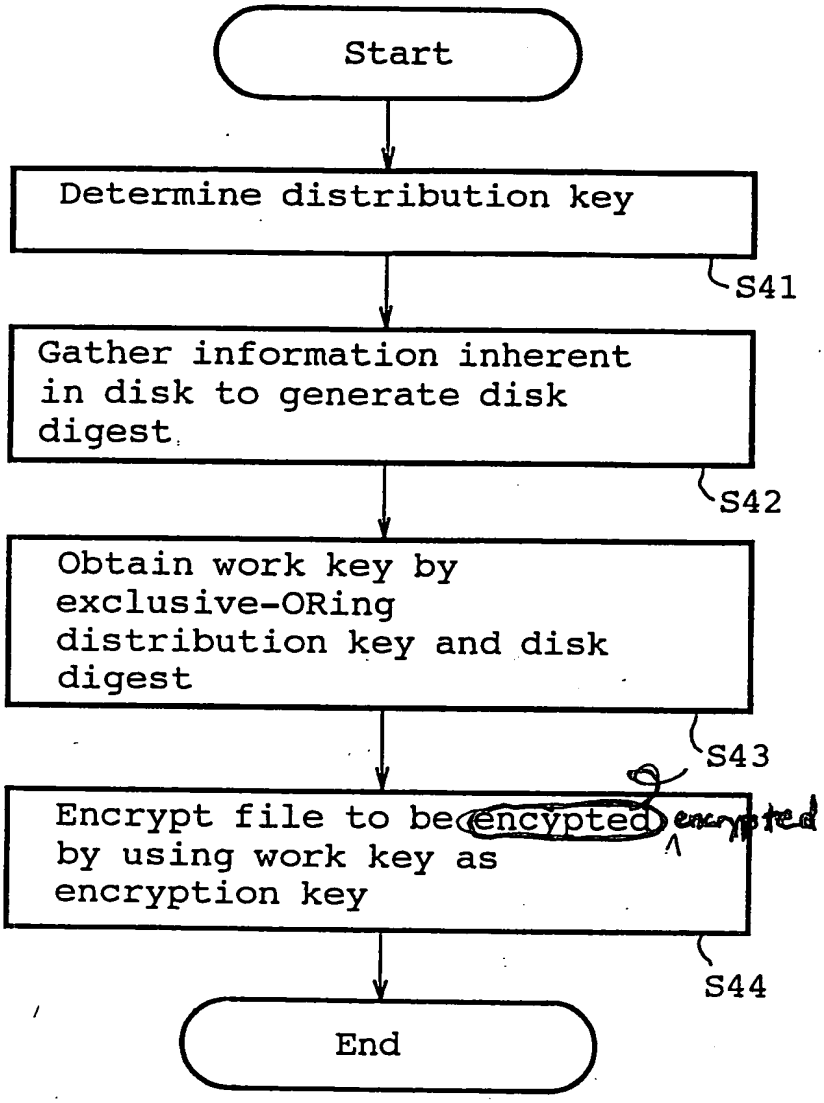
Approved 24 Oct 2003 JWS

FIG. 10



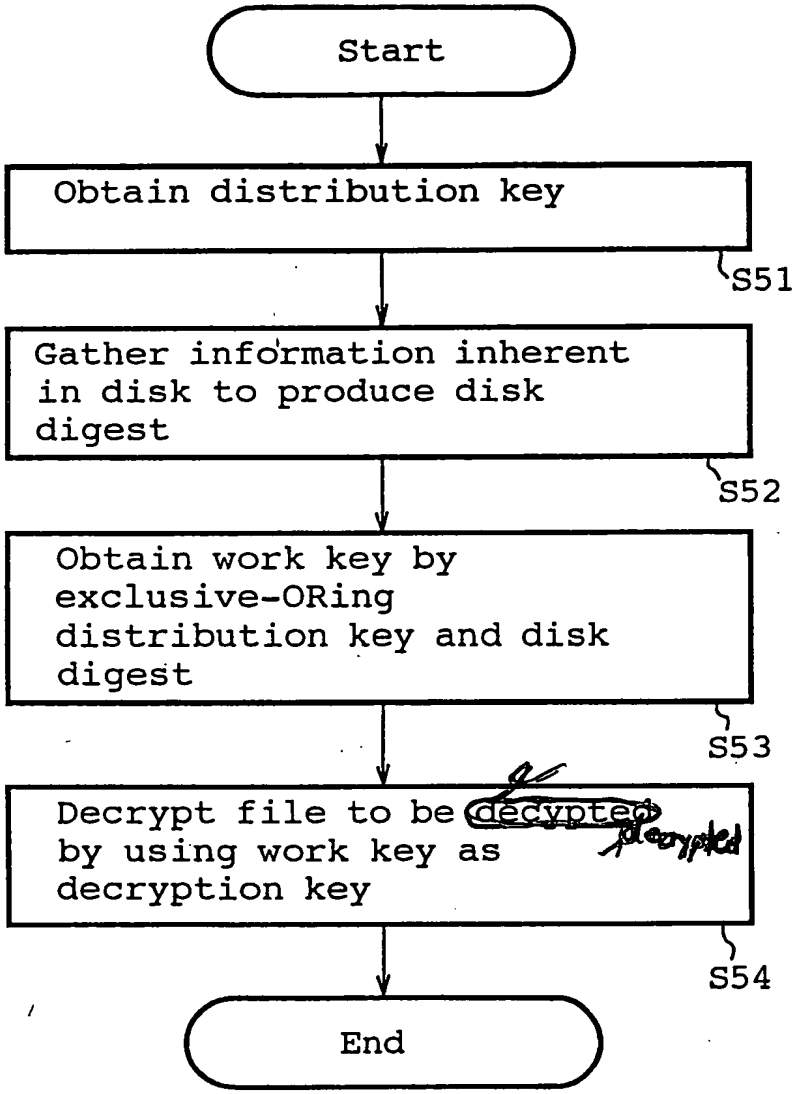
Approved
24 Oct 2002

FIG. 11



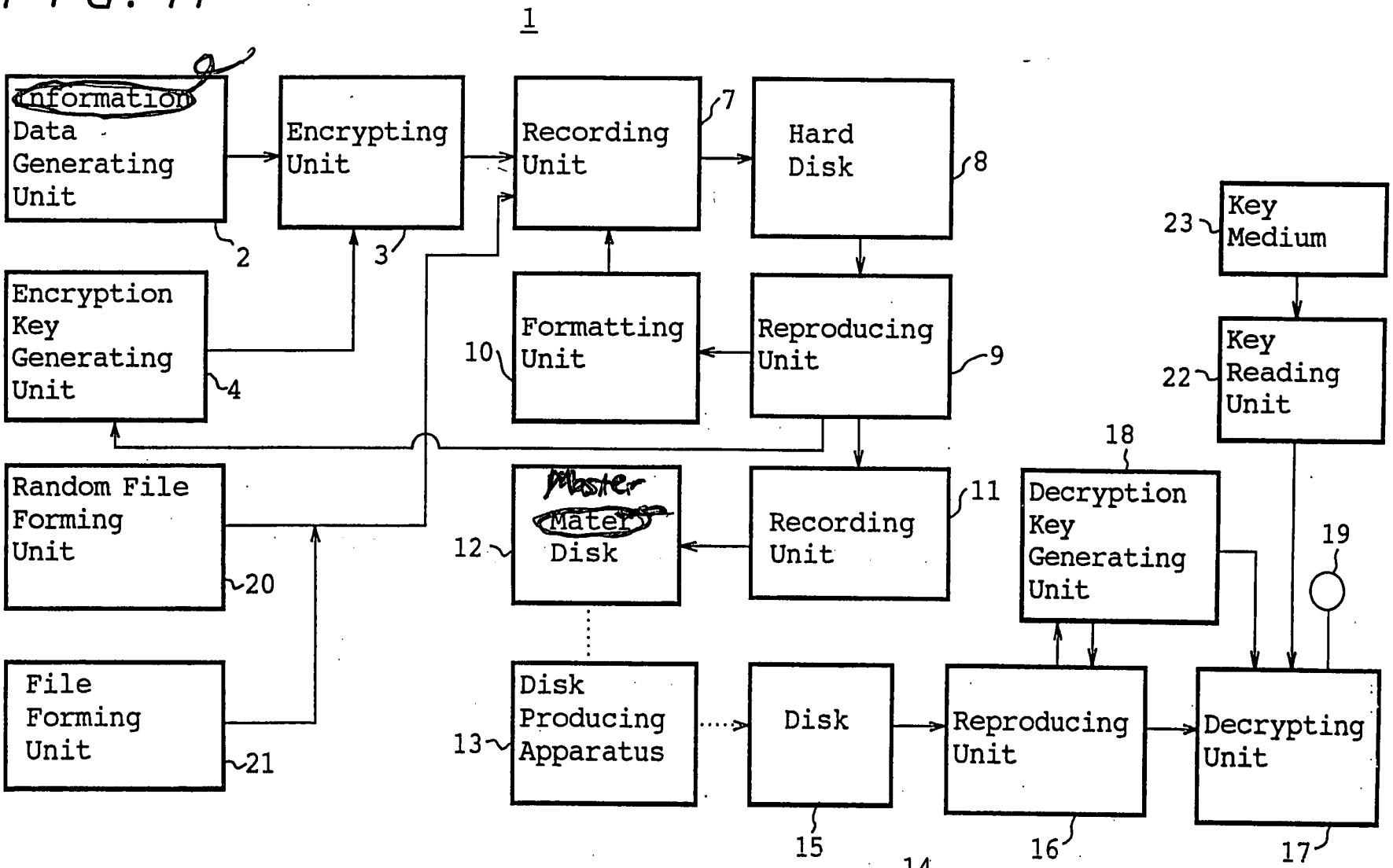
Approved
24 Oct
2003
JWS

FIG. 12



Approved
24 Oct 2003
JWS

FIG. 14



Approved
24 Oct 2005
TWS